

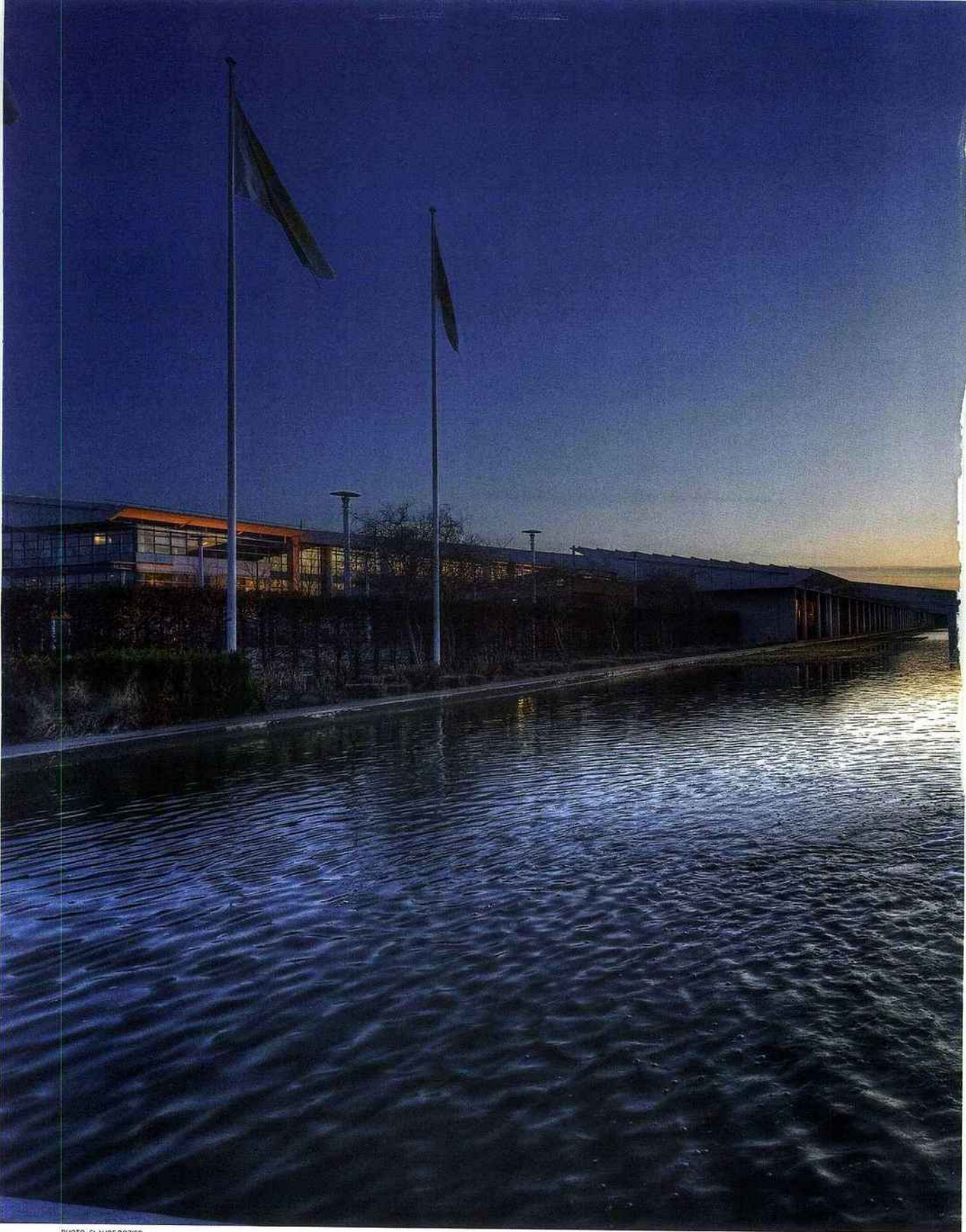


PHOTO: CLAUDE ROZIER



Concurrence

L'INDUSTRIE, UN NID D'ESPIONS

L'affaire d'espionnage présumé chez Renault est loin d'être isolée. Toutes les entreprises, quels que soient leur taille et leur domaine d'activité, risquent, un jour ou l'autre, de déplorer la perte d'informations importantes. Exemples et parades.

LA RÉDACTION

VOUS ÊTES CONCERNÉS
• Dirigeants d'entreprises
• Cadres en déplacement
• Techniciens en relation avec les fournisseurs
• Salariés tuteurs
• Ingénieurs intervenants à l'extérieur

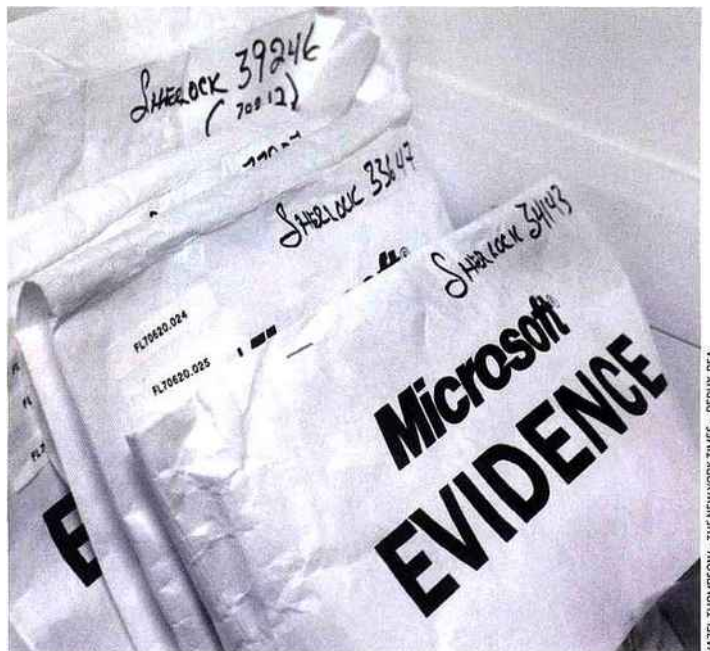
Et si l'affaire d'espionnage dévoilée par Renault était un mal pour bien ? Après le dépôt d'une plainte, une enquête de la Direction centrale du renseignement intérieur (DCRI) devra faire la lumière sur le « système organisé de collecte d'informations » dénoncé par Patrick Pelata, le numéro deux du constructeur. Sans présager des conséquences de cette enquête, l'affaire Renault, comme on l'appelle, devrait déclencher une prise de conscience salutaire pour de nombreux chefs d'entreprise. « Cela nous incite à renforcer nos moyens et méthodes pour défendre notre savoir-faire. Nous envisageons la nomination d'un responsable de la sécurité qui ira se former dans les stages organisés par la DCRI et la gendarmerie », explique Bruno Grandjean, le président du directoire de Redex, un fabricant de réducteurs qui réalise 90 % de son chiffre d'affaires à l'exportation. Loin d'être une affaire de grands groupes, l'espionnage industriel menace tout un chacun. Un concurrent, qui ne peut obtenir des informations de manière transparente, peut être tenté de les obtenir de façon déloyale... quand ce n'est pas en recourant à des moyens illégaux. Les spécialistes de l'intelligence économique parlent ainsi d'information blanche, pour celle que n'importe qui peut glaner dans la presse ou sur internet, d'information grise, à laquelle on accède en recourant à un procédé malhonnête, et d'information noire, obtenue par la corruption et le vol notamment. Revue de détail des menaces et des parades. ■

Le Technocentre Renault de Guyancourt (Yvelines). Trois salariés du constructeur ont été mis à pied, accusés d'avoir divulgué des informations sur le programme électrique.

QUAND IL SUFFIT DE SE SERVIR...

Journaux, magazines, comptes déposés aux greffes des tribunaux de commerce, presses d'entreprise, internet, réseaux sociaux... vous n'imaginez pas toute l'information qui est disponible concernant votre entreprise ! Avec internet, la liste des outils pour recueillir des informations sur un industriel, une technologie, un produit ou un secteur d'activité ne cesse de s'allonger. Le dernier cheval de Troie en date ? Les réseaux sociaux. Ils sont de vraies mines d'information. Sur LinkedIn ou Viadeo, un chercheur avisé peut repérer des infos en or. Il lui suffit de compléter un puzzle. Plus il trouve de morceaux qu'il peut assembler, plus la probabilité est forte qu'il s'approche d'une image exacte. « En soi, ce ne sont pas les informations sur tel ou tel profil qui compte, mais la compilation qui donne du sens. On peut ainsi reconstituer un organigramme, connaître un fournisseur ou estimer le budget d'un service », explique Pierre-Jacquelin Romani, directeur adjoint du groupe Geos Business Intelligence, spécialisé dans la gestion des risques.

Parfois, les informations peuvent se retrouver sur la place publique par volonté de... communiquer ! Il y a quelques années, un groupe de travail chez Sew-USocom, un gros fabricant de moteurs et de motoréducteurs, avait décrit dans un journal interne comment fiabiliser un process avec très peu de moyens. La publication a été évitée de justesse par



Microsoft est l'un des groupes les plus actifs dans la lutte contre l'espionnage industriel.

Bientôt une loi pour protéger vos secrets

Les pouvoirs publics n'ont pas attendu l'affaire présumée d'espionnage chez Renault pour vouloir légiférer sur le sujet. Le délégué interministériel à l'intelligence économique, Olivier Busquen, travaille à l'élaboration d'un projet de loi depuis le début de l'année 2010. Deux volets sont envisagés. Primo, la possibilité pour les sociétés d'estampiller des informations « Confidential entreprise » afin de leur donner une valeur juridique. Secundo, sur un mode répressif, le recours à des poursuites au pénal et au civil à l'encontre des entreprises soupçonnées de violation du secret des affaires. « C'est un processus important à mettre en place, précise Olivier Buquen. Les chefs d'entreprise que j'ai rencontrés ces derniers jours

m'ont confié ne pas toujours soupçonner l'étendue des menaces. Or, pour une entreprise, dès qu'un savoir-faire est différenciant, elle est potentiellement menacée. » Le projet de loi n'est pas encore tout à fait au point. Fin 2010, le ministère de l'Industrie en a fait parvenir les grands principes juridiques au Conseil d'État, qui devrait se prononcer dans les prochaines semaines. « On peut craindre avec cette loi une certaine opacité dans la gestion des entreprises, estime Hervé Séveno, président de la Fepie (syndicat français de l'intelligence économique). Il faut déterminer de façon plus précise la notion de "Confidentiel entreprise". » La loi pourrait être votée d'ici à la fin de l'année. ■ O. C. E. O. J.

l'intervention d'un membre du comité de rédaction au fait des problématiques de sécurité. Sans son veto, les concurrents n'auraient eu qu'à lire le magazine pour acquérir un savoir-faire différenciant. « Nos chimistes sont très attentifs à ne jamais laisser de trace écrite de formule des médicaments, raconte, de son côté, Loïc Mazurell, le PDG d'ExonHit Therapeutics (biotechnologies, 70 salariés). Lorsqu'ils travaillent à l'amélioration d'une formule chimique, ils dessinent un pont sulfurique dans le vide pour ne pas que cela puisse être relié à un produit. Nous sommes très attentifs à ce qu'on ne voit jamais une formule écrite, même en partie de l'un de nos produits. »

Pour éviter que des informations sensibles ne tombent entre de mauvaises mains, d'autres industriels limitent leur diffusion en interne. « Tout le monde n'a pas besoin de tout savoir de l'état d'avancement d'un projet, explique Luc Renouil, le directeur du développement de Bertin Technologies (santé, énergie et défense). On essaie donc de donner juste l'information nécessaire et suffisante aux équipes pour qu'elles puissent mener à bien leurs travaux. Même si ce cloisonnement a un coût en termes de réseau, de relationnel entre le chef et son équipe... Il faut former les équipes à ce type de fonctionnement. »

La communication verbale des salariés reste, toutefois, difficile à contrôler. « Il peut arriver à un ingénieur, en voulant se vanter d'une avance technologique, de dévoiler dans ses discussions, sur un salon, des informations stratégiques pour l'entreprise, explique Patrick Henry, le directeur général de Velan, un fabricant de pompes pour le nucléaire. Il faut privilégier l'éducation du personnel. La sécurité est un problème de culture d'entreprise. Elle doit être un état d'esprit permanent. » Les commerciaux doivent apprendre à préparer

Le dernier cheval de Troie ? Les réseaux sociaux qui sont une mine d'informations.

et à débriefeur leurs rendez-vous dans un lieu fermé, et traiter, en public, des sujets sans risque.

La SSII Sogeti annexe au contrat de travail de ses salariés une charte de sensibilisation à la sécurité. Des piqures de rappel sont réalisées sur l'intranet. Les documents enregistrés sur les micro-ordinateurs portables sont chiffrés. La perte d'un ordinateur, non sécurisé, peut avoir de lourdes conséquences. « Il y a quelques mois, une grande entreprise du BTP s'est fait voler un micro-ordinateur portable dans une baraque de chantier. Ce dernier contenait les plans de la prison qui était en cours de construction », raconte, à titre d'exemple, Edouard Jeanson, responsable pratiques sécurité chez Sogeti.

Les parades

Chaque entreprise doit déterminer le type d'informations qu'elle souhaite garder confidentielles, en contrôler et en limiter la diffusion. La destruction des documents sensibles doit avoir lieu dès que possible. Le réseau informatique interne peut être déconnecté physiquement du web. Attention au Wi-Fi ouvert dans certains lieux publics : des restrictions sur les objets nomades (ordinateurs portables, smartphones, clés USB...) sont toujours possibles. Le « passeport de conseils aux voyageurs » de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est particulièrement bien fait... et utile.

QUAND LA ROUERIE LE DISPUTE À LA MALHONNÊTÉTÉ...

Il y a quelques années, un recruteur s'est installé non loin des bureaux toulousains d'Airbus. Alléchés par des offres d'emploi rémunératrices, les cadres de l'avionneur y défilaient pour passer des entretiens d'embauche qui ne débouchèrent jamais. Et pour cause ! Le recruteur n'existait pas. On a soupçonné un concurrent d'Airbus d'être venu ainsi récolter des informations utiles. La méthode, perverse, a tout pour réussir : un cadre à l'affût d'un nouveau poste peut être bavard pour séduire son futur employeur. Le procédé est la fois déloyal et malhonnête...

Chez les pétroliers et parapétroliers, les salariés sont sensibilisés à la question des clés USB. Régulièrement, des personnes malveillantes laissent traîner des clés sur le sol des parkings destinés aux salariés d'une des entreprises du secteur. Si un salarié en ramasse une et la branche sur son ordinateur pour vérifier ce qu'elle contient, un virus peut alors se déployer sur le réseau de la société et des informations être transmises vers l'extérieur. Des campagnes incitent



En 2005, la chinoise Li Li Whuang, stagiaire chez l'équipementier automobile Valeo, fut soupçonnée d'espionnage industriel. Elle a été condamnée pour abus de confiance.

les salariés à ne jamais utiliser des clés USB dont ils ne connaissent pas l'origine.

Il y a encore plus vicieux ! Sunaero, une PME de 17 salariés basée à Genay, près de Lyon (Rhône), détient une expertise unique dans la détection et la réparation des fuites de carburant sur les avions civils et militaires. Les armées françaises et américaines utilisent ses équipements. Sa technologie sensible, développée sur demande de la Délégation générale à l'armement, lui permet de bénéficier d'un soutien de la Direction de la protection et de la sécurité de la défense et de la DCRI. Quand des offres commerciales s'offrent à elle, Sunaero y regarde à deux fois. « En juin 2010, un laboratoire de recherche de Singapour nous a contacté pour évaluer notre technologie de réparation par polymérisation rapide. Leurs questions très ciblées ont éveillé notre méfiance, explique Thierry Regond, le vice-président. Nous avons fait appel à une société de renseignements privée. Après enquête, il s'est avéré

que ce laboratoire était en fait missionné par un institut de recherche privé, lui-même en relation directe avec un grand donneur d'ordres. Suite au premier rendez-vous et malgré leurs relances, nous avons stoppé tout contact. »

Les transferts de technologie sont à surveiller de très près, confirme Robert Moor, le PDG de Protex International (chimie de spécialités). « Chez nous, ils se font en limitant certaines informations stratégiques, précise le PDG. Pour ce qui est des produits intermédiaires, nous ne divulguons pas la composition de nos produits. Pour certains matériels de production, les plans ne sont pas transférés et seul est donné le matériel avec son mode d'emploi. Le degré de confidentialité varie également avec le pays où se trouve la filiale. »

Depuis septembre 2010, Arc International s'est doté d'un poste de directeur de la propriété industrielle et intellectuelle. Auparavant, la fonction était occupée par le directeur juridique du groupe. Arc a recruté un ancien responsable de LVMH, Thomas Striffling, spécialiste des problèmes de contrefaçons et de propriété industrielle. Ses missions : la protection des innovations technologiques sur de nouveaux matériaux, via des enveloppes solos (solution plus confidentielle que le dépôt de brevets), la protection des

Les transferts de technologie sont à surveiller de très près.

PIERRE VERDY/AFP OR



“Les pays émergents ont mis en place un système organisé et légal”

OLIVIER DARRASON

Président de la Compagnie européenne d'intelligence stratégique (CEIS)

L'espionnage industriel, est-ce toujours une affaire de corruption ou de barbouze ?

Non. Le cas de Renault, s'il est avéré, n'est pas représentatif des risques auxquels sont exposées les entreprises françaises. L'espionnage industriel est de plus en plus remplacé par des méthodes légales et organisées. Des pays émergents mettent en place à haut niveau un système de transfert de technologies, en fonction d'un plan préétabli. Cela passe par des achats de technologies, des coopérations scientifiques très ciblées, où l'on vise une équipe de recherche bien identifiée. Il y a aussi la captation des cerveaux, consistant à offrir des postes dans des universités ou des centres de recherche.

Quels sont ces pays ?

Il y a tous les grands pays émergents, comme la Chine et le Brésil. Mais pas seulement. Des pays comme les Émirats arabes unis, le Qatar et la Malaisie sont de plus en plus actifs. Ils ont une vraie et « intelligente » stratégie pour organiser ces transferts de technologie. En revanche, la Corée du Sud est passée du camp des demandeurs de technologie à celui des « fournisseurs », sans avoir abandonné sa « quête » extérieure. Un nombre croissant d'échanges a lieu directement entre pays du Sud.

Comment affronter cette menace ?

Il faudrait d'abord être conscient de ce mouvement ! Ensuite, il faudrait mieux accompagner les PME, qui sont les plus exposées. Elles développent parfois des technologies très sensibles et leurs besoins de financement sont importants. ■ PROPOS RECUEILLIS PAR G. L.-B.

créations esthétiques et le renforcement des contrôles, en particulier en Asie.

« La Chine est l'une des zones qui produit le plus de contrefaçons, en particulier sur les formes et les décors. Il y a parfois des décalages entre les discours tenus par les autorités du pays et la réalité observée sur le terrain. C'est très difficile de contrôler tout le territoire. Nous essayons d'augmenter nos moyens de veille sur place, grâce à la présence de nos commerciaux et responsables marketing, explique Thomas Striffling. La foire de Canton, qui a lieu deux fois par an, est un lieu incontournable pour voir tout ce qui est vendu et fabriqué en Chine. C'est un bon moyen d'identifier les contrefaçons. »

Les parades

Il faut sensibiliser le personnel. Ce qui revient très souvent à fermer les portes... La surveillance des allées et venues dans l'entreprise est un minimum. Les informations données aux fournisseurs doivent être limitées. Certaines entreprises travaillant dans des secteurs sensibles équipent leurs collaborateurs de deux ordinateurs, l'un fixe relié à un réseau fermé, l'autre, portable, pour accéder à un réseau plus ouvert. Certains membres du ministère de la Défense sont même équipés de trois postes différents.

**Augmenter les
moyens de veille à
l'étranger pour
mieux lutter contre
la contrefaçon.**

QUAND TOUS LES MOYENS SONT BONS...

La fin justifie les moyens pour certains de vos concurrents. Pour porter atteinte à une organisation, obtenir les secrets d'un nouveau produit ou les détails d'une stratégie, certains industriels n'hésitent pas à franchir la ligne rouge. Vols, corruption, espionnage, intimidations... tous les coups sont permis pour atteindre son but. «Pour déstabiliser un concurrent, on peut salir l'image d'un produit, dénigrer un dirigeant ou même déstabiliser une assemblée générale avant un vote essentiel», souligne Christian Harbulot, le directeur de l'École de guerre économique.

La PME suisse Ethical Coffee Company (ECC), qui s'est attaquée au monopole de Nestlé sur les dosettes Nespresso, a dû subir les pressions du géant de l'agroalimentaire. Si ce dernier a porté l'affaire sur le terrain juridique, pour Jean-Paul Gaillard, le PDG d'ECC, «Nestlé s'est procuré d'une manière illicite un certain nombre de nos capsules. Nous en avons la preuve». Ces informations, obtenues illégalement selon ECC, lui aurait permis de faire réaliser, le 23 juin, une action en saisie-contrefaçon des dosettes d'ECC chez son sous-traitant de Chambéry (Savoie), les Cafés Folliet. «Sur place, ils ont tenté d'intimider des personnes pour obtenir l'adresse de nos fournisseurs alors que cette demande ne figurait pas dans l'ordonnance du juge», s'indigne aujourd'hui encore le dirigeant qui a porté plainte contre X en France pour espionnage industriel... Tout en restant réaliste : «Rien ne



Marwan Arbache à sa sortie du tribunal en mai 2010. L'employé de Michelin aurait tenté de vendre des informations confidentielles au concurrent japonais Bridgestone.

peut être sécurisé à 100% lorsqu'une tentative émane de quelqu'un ayant d'aussi gros moyens.»

Les risques de vol de données se sont accrus avec l'internationalisation des entreprises. À l'étranger, le salarié est loin de son directeur sécurité. Surtout, la culture des salariés est différente d'un pays à l'autre. Dans certains pays, la transmission des informations est naturelle, alors qu'ailleurs, la rétention est la règle. «Il faut donner un niveau

QUATRE PARADES FACE AU RISQUE INFORMATIQUE

ANTIPIRATES



Outils Firewall et anti-intrusion

Éditeurs Symantec, McAfee, Aruba...

Notre conseil Installer et tenir à jour le duo de logiciels «anti-espion» et «pare-feu», pour limiter le risque d'intrusion dans le réseau de l'entreprise. Et, pour limiter la fuite des données, désactiver les connecteurs USB des micro-ordinateurs et choisir des modèles sans graveur de DVD.

ANTI-INTRUSION



Outils VPN, réseau privé virtuel

Éditeurs CheckPoint, Cisco, HP...

Notre conseil Toujours choisir un réseau Wi-Fi avec une clé de chiffrement WPA2, les clés WEP et WPA étant totalement inefficaces face aux pirates, même amateurs. Interdire l'accès à internet depuis un réseau Wi-Fi public et obliger l'utilisateur à passer par le serveur de son entreprise via un «réseau privé virtuel» (VPN).

ANTIFIUITES



Outil Chiffrement à la volée

Éditeurs TrueScript (libre), GNU Privacy Guard, Sophos...

Notre conseil Équiper les micro-ordinateurs portables, comme les smartphones, d'un logiciel de chiffrement à la volée, paramétré par défaut. Pour les documents confidentiels, penser à interdire l'impression, l'envoi à une tierce personne, et prévoir la destruction automatique, dans les préférences, des PDF, après un certain temps.

ANTIVOL



Outil Traqueur

Éditeurs Prey, Lalarm...

Notre conseil En cas de perte ou de vol, des systèmes existent pour bloquer, voire détruire le disque dur d'un micro-ordinateur portable ou l'espace de stockage d'un smartphone, dès la première tentative de connexion à internet. On peut aussi localiser l'appareil. Des parades à installer en standard, notamment sur les smartphones.

Un outil de légitime défense

C'est grâce à la « procédure déontologique » mise en place en 2007 que Renault aurait appris les fuites. Un salarié a donc vraisemblablement utilisé ce dispositif pour dénoncer un manquement à l'éthique. Aux États-Unis, depuis la loi Sarbanes-Oxley, adoptée en 2002 après l'affaire Enron, un système d'alerte éthique (whistleblowing) est obligatoire dans toutes les entreprises cotées. Les groupes français s'y mettent doucement,

mais ne souhaitent pas communiquer. « Toutes les entreprises du CAC 40 en sont sans doute dotées », estime un expert. Numéro vert ou boîte mail, le système soulève la méfiance voire l'hostilité des syndicats, qui y voient un encouragement à la délation. La CGT de la métallurgie a par exemple attaqué le système mis en place par Dassault Systèmes. La Cour de cassation lui a donné raison en décembre 2009, invoquant une atteinte à la liberté

d'expression, et un non-respect des règles édictées par la Commission nationale informatique et libertés (Cnil). « Le système d'alerte fait partie de la légitime défense de l'entreprise, analyse Bernard Besson, collaborateur du Haut responsable à l'intelligence économique de 2003 à 2010. Mais, dans la mesure où il touche aux libertés individuelles, il doit être élaboré avec les salariés et dans le respect de la protection des données personnelles. » ■ C. M.

de confidentialité à chaque information, que chacun sache dans quelle mesure il peut ou non en parler, et avec qui», conseille Olivier Hassid, le directeur du Club des directeurs de sécurité des entreprises (CDSE).

La menace provient, très souvent, de l'intérieur même des entreprises. « C'est le salarié, le technicien ou l'ingénieur, qui part avec la technologie de la société, soit pour créer son entreprise, soit pour travailler pour un concurrent », observe Frédéric Saffroy, avocat associé chez Alberion. La plupart des dossiers se règlent discrètement, entre avocats. « Pour les vols d'informations et de technologies, cela peut finir au pénal. Mais généralement, cela intervient de manière discrète, sans communication des avocats. On essaie d'éviter la sphère pénale, à la fois en termes d'efficacité et en termes de discrétion. »

Le « cas » Renault met en évidence, s'il en était besoin, ce maillon faible : le facteur humain. « La loyauté des dirigeants ou des salariés doit être un ressort de développement de l'entreprise. La loyauté joue si elle est réellement réciproque, note Luc Renouil, directeur du développement de Bertin Technologies. L'affaire Renault nous amène à reconsidérer nos pratiques et à balayer devant notre porte. Nos contrats de travail sont-ils correctement conçus en termes de propriété intellectuelle et de secret ? L'intérêt du salarié et celui de l'entreprise y sont-ils bien retranscrits ? »

Les parades

Il faut identifier les informations dont l'entreprise a besoin, et celles qui peuvent intéresser. Les spécialistes de l'intelligence économique recommandent de former des gestionnaires des risques, qui s'occupent entre autres de l'espionnage industriel. Il faut utiliser la mémoire de l'entreprise, ses réseaux, pour identifier les moments risqués, les entités qui pourraient avoir recours à des méthodes illégales. Une bonne politique de prévention consiste à écouter les cadres. Ils doivent être considérés, pour devancer les situations personnelles de fragilité. L'intelligence économique se fait avec tous les salariés de l'entreprise. ■